



**DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR MOBILITY COMMAND**

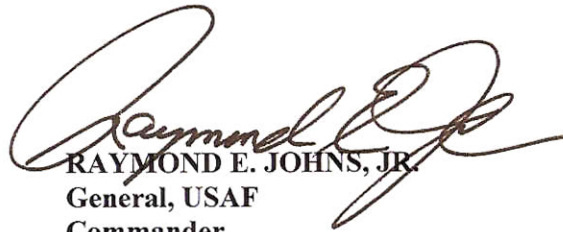
14 June 2010

**MEMORANDUM FOR ALL AMC AIRMEN**

**FROM:** AMC/CC  
402 Scott Drive, Unit 3EC  
Scott AFB IL 62225-5310

**SUBJECT:** Guidance for Airmen Communicating Via the Internet

1. As the Air Force opens the network to Internet-based capabilities, including social networking sites, we must ensure we strike a balance between security and appropriate access. While these new tools will allow Airmen to communicate more effectively, it is imperative that we protect the network and safeguard information related to the mission.
2. When using Internet-based capabilities, the same basic rules we've all learned apply for any public forum, whether on or off the Internet:
  - Abide by Operations Security (OPSEC) rules and protect Critical Information.
  - Conduct yourself professionally at all times.
  - Protect the Air Force Network from malicious attacks.
  - Use government communication systems for official and authorized purposes only.
  - If you are unsure, contact your supervisor, your unit OPSEC manager, or your local Public Affairs Office.
3. In today's age of Internet media, we have access to social networking sites which allow us to easily communicate with other Airmen, our families and friends, and people throughout the world. As Airmen, we must continue to uphold the highest standards of conduct and professionalism while utilizing these Internet resources.
4. The Internet is becoming the world's primary source of information, and our Airmen are active participants. It is more important than ever to promote a climate of responsible public communication. You represent the Air Force anytime you communicate online and, therefore, are always on the record and must always represent our core values: Integrity first, Service before self, and Excellence in all we do.
5. Please ensure every AMC Airman reads and understands the attached "AMC Social Media Guidance."

  
RAYMOND E. JOHNS, JR.  
General, USAF  
Commander

**Attachment:**  
AMC Social Media Guidance



# Social Media Guidance

---

## Air Mobility Command

JUNE 2010

## 1. BACKGROUND

As the Air Force opens its network to Internet-based capabilities, including social networking sites, we must strike a balance between safeguarding the mission and maintaining a safe and controlled network to defend against malicious activity while allowing Air Mobility Command Airmen to have appropriate access.

- 1.1. This guidance applies to all AMC Airmen, including military personnel and Department of Defense civilian employees and contractors.
- 1.2. Internet-based capabilities are defined as all publicly accessible information capabilities and applications available across the Internet in locations not owned, operated or controlled by the Air Force, Department of Defense, or the Federal Government. Internet-based capabilities include collaborative tools such as social networking services, user-generated content, social software, e-mail, instant messaging, and discussion forums.
- 1.3. In today's age of Internet media, we have access to Internet-based capabilities which allow us to easily and quickly share information, professionally or personally, with people throughout the world. Airmen, both military and civilian, need guidance, tools and empowerment to communicate with this medium. This includes Airmen sharing their personal and professional stories with the global audience while remaining vigilant to not harm fellow warfighters, endanger the mission, or speak outside their area of expertise.
- 1.4. The Air Force fully supports Airmen communicating appropriately via social networking sites; however, because Operations Security (OPSEC) violations, viruses and social engineering (i.e., the act of manipulating people into performing actions or divulging confidential information) are common on all social networking sites, guidance and education are essential in combating most threats these sites present and preserving/protecting our combat capability.

## 2. INTERNET USE

It is important all Airmen – military personnel and DOD civilian employees and contractors – understand the three types of Internet use that this guidance applies to (official; authorized personal; and unofficial/off-duty):

- 2.1. **Official use.** Includes official activities conducted on DOD and non-DOD Internet sites (i.e., Websites, blogs, social networking services, etc.). These services are primarily used by commanders and/or their appointed representatives and are geared toward communicating directly with Airmen, their families and the general public.
  - 2.1.1. External official presence using Internet-based capabilities is allowed. An external official presence is defined as official public affairs activities conducted on non-DOD Internet sites (e.g., AMC commander on Facebook, Chairman of the Joint Chiefs of Staff on Twitter).
- 2.2. **Authorized personal use.** Includes the limited authorized personal use of Internet-based capabilities on government-owned computer systems.
  - 2.2.1. All Airmen – military personnel and DOD civilian employees and contractors – must understand that DOD computer systems are provided only for official U.S. Government use and limited authorized personal use.

- 2.2.2. Limited authorized personal use must be of reasonable duration and frequency that has been approved by supervisors and does not adversely affect performance of official duties, overburden systems, or reflect adversely on the Air Force. In deciding whether to approve particular limited personal uses of government systems, supervisors should consider whether Websites or social network sites contain offensive or inappropriate material, even if not endorsed by the Airman, and whether alternative channels for official or unofficial communications may be more appropriate under the circumstances.
- 2.2.3. DOD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized; for management of the system; to facilitate protection against unauthorized access; and to verify security procedures, survivability, and operational security.
- 2.2.4. Using a government-owned computer for other than official or limited authorized personal use may result in adverse administrative or disciplinary action.
- 2.2.5. For a more complete description of “appropriate use,” see AFI 33-129, Paragraph 2, and DOD 5500.7-R (Joint Ethics Regulation), Paragraph 2-301.
- 2.3. **Unofficial/off-duty use.** Includes the use of personal Websites and social networking services (i.e., blogs, Facebook, Twitter, YouTube, etc.) by Airmen in an unofficial, off-duty capacity, using a non-government-owned computer or device (i.e., home computer, personal mobile device, commercial network connection, etc.).
  - 2.3.1 Airmen must remember that they are ALWAYS Airmen and their conduct online, whether on or off-duty, communicates Air Force values, and their actions, positive or negative, reflect not only on themselves, but on the entire service.

### 3. OPERATIONS SECURITY GUIDANCE

The following guidance is for Airmen who are discussing the Air Force online, whether in an official, authorized personal, or unofficial/off-duty capacity:

- 3.1. Do not discuss or post classified, For Official Use Only (FOUO), Controlled Unclassified/Sensitive Information, Critical Information, and/or personally identifiable information.
- 3.2. Although some information is not classified, sensitive information may provide small pieces to a larger puzzle that would be useful to our adversaries. Basic to the OPSEC process is determining what information, if available to one or more adversaries, would harm your organization’s ability to effectively carry out its operations or activities. In other words, seemingly innocent information, when combined, may reveal valuable intelligence to our enemies.
- 3.3. Airmen must not post information included on the AMC or unit Critical Information List (CIL). Critical information consists of information and observable actions about unit activities, intentions, capabilities, or limitations that must be controlled to prevent an adversary from gaining a significant military, economic, political, or technological advantage. See your unit OPSEC manager for more details.

- 3.4. Do not reveal information that could suggest troop movements, system information, weapons information, military organization, or other valuable intelligence to a potential adversary. In brief, do not discuss specific names, dates, times or locations in relation to Air Force operations.
- 3.5. When posting duty-related information or images, check for indicators that may divulge sensitive information. Additionally, when posting images, inspect the background and any reflective surfaces for indicators, including names, dates, times or locations related to Air Force operations.

#### **4. APPROPRIATE ONLINE ACTIVITY/BEHAVIOR**

- 4.1. Do not post defamatory, libelous, vulgar, obscene, abusive, profane, threatening, hateful, racially, ethnically, or otherwise offensive or illegal information or material.
- 4.2. Do not upload videos you did not create, or use content in your videos that someone else owns the copyright to, such as music tracks, snippets of copyrighted programs, or videos made by other users, without necessary authorizations.
- 4.3. Be cautious of how something can be interpreted by the public. If there is any concern on how it will be interpreted, it should not be posted.
- 4.4. Do not cross the line between funny and distasteful.
- 4.5. Do not post images or videos of persons detained by U.S. military personnel.
- 4.6. When photographing military personnel in uniform, ensure all safety and uniform dress and appearance policies and guidelines are adhered to (i.e., personal protective gear is worn, restricted area badges removed, uniform is worn correctly, etc.).
- 4.7. Do not post photographs of military personnel in social situations that highlight or promote the use of alcoholic beverages or other situations that may bring discredit to the Air Force.
- 4.8. During humanitarian operations:
  - 4.8.1. Respect the people and conditions within that area of operations; it is their home and we are guests.
  - 4.8.2. Remain sensitive to the people you encounter in the sharing of their stories; the U.S. military is there to help them, not exploit them.
  - 4.8.3. Avoid photographing or recording images that would reduce the dignity of the people involved, or would be deemed exploitive, or photos of those deceased or suffering.
  - 4.8.4. Every action should reflect our nation's compassion and commitment.
- 4.9. Do not forge or otherwise manipulate identifiers in posts in an attempt to disguise, impersonate, or otherwise misrepresent your identity or affiliation with any other person or entity.
- 4.10. When writing about the Air Force on a personal Web site or blog, identify to your readers that the views expressed are yours alone and do not necessarily reflect the views of the Air Force.

Use a disclaimer such as: “The postings on this site are my own and don’t necessarily represent Air Force positions, strategies, or opinions.”

- 4.11. Airmen discussing issues related to their career field or a personal experience is acceptable, but they should be careful not to imply that they have expertise in areas for which they have no first-hand, direct background or knowledge.
- 4.12. Do not use any words, logos or other marks that would infringe upon the trademark, service mark, certificate mark, or other intellectual property rights of the owners of such marks without the permission of such owners.
- 4.13. Do not post any information that would infringe upon the proprietary, privacy, or personal rights of others.
- 4.14. The activities listed below involving the use of government-provided computer hardware or software are specifically prohibited:
  - 4.14.1. Use of Federal government communications systems for unauthorized personal use.
  - 4.14.2. Uses that would adversely reflect on the DOD or the Air Force, such as chain letters, unofficial soliciting or selling, except on authorized systems established for such use.
  - 4.14.3. Unauthorized storing, processing, displaying, sending, or otherwise transmitting prohibited content. Prohibited content includes: adult content, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the basis of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin, sexual orientation), gambling, illegal weapons, militancy/extremist activities, terrorist activities, and any other content or activities that are illegal, inappropriate, or offensive to fellow users or the public.

## 5. PROTECTING THE AIR FORCE NETWORK

Adversaries continuously attempt to infiltrate Air Force networks and systems trying to steal, compromise, degrade or destroy information, disrupt networks or communications, or deny service. All Airmen must take precautions to ensure we protect our networks. In addition to protecting information, all Airmen must do their part to protect the Air Force Network (AFNET) from malicious attacks (i.e., viruses, Trojans, worms, spyware, etc.), which can significantly disrupt operations.

- 5.1. When visiting social networking sites, beware of links, downloads and attachments, just as you would in e-mails.
- 5.2. To prevent unknowingly opening the Air Force network to a virus, spyware or other malware, do not visit questionable sites from a government computer.
- 5.3. Beware of “apps” or plugins, which are often written by unknown third parties who might use them to access your data.
- 5.4. Do not download or install freeware/shareware or any other software product without Designated Approving Authority (DAA) approval.
- 5.5. Do not permit anything to run on your computer that you did not install or that you do not understand – it could be malicious code.

- 5.6. Ensure your passwords are unique; use special characters and numbers when possible.
- 5.7. Ensure your passwords are sufficiently hard to guess.
- 5.8. Ensure your passwords are protected; do not share your passwords with anyone.

## 6. ADDITIONAL GUIDANCE

- 6.1. Everyone has a responsibility to protect themselves online. Air Force personnel should take steps to ensure operations security and safeguard personally identifiable information at work and at home.
- 6.2. If you or someone you know posts information that violates the above guidance, ensure the information is quickly removed, and immediately notify your supervisor and/or your local Public Affairs office.
- 6.3. To continue safeguarding the Air Force network, as well as the security and privacy of all Air Force personnel, reference the following:
  - [http://www.iooss.gov/sns\\_safety\\_check.pdf](http://www.iooss.gov/sns_safety_check.pdf): OPSEC and Social Networking Safety check list
  - <http://socialmedia.defense.gov/index.php/games/>: DOD Social Media Hub
  - <http://www.stratcom.mil/snstraining/index.html>: USSRATCOM Social Network Training
  - <http://www.af.mil/shared/media/document/AFD-091210.pdf>: Social Media and the USAF
  - [Air Force Instruction 33-129, Section 2](#): Use of Internet Resources by Government Employees
  - [Air Force Instruction 35-107](#): Public Web Communications
  - [Air Force Instruction 35-113, Paragraph 15](#): Social Media
  - [DOD 5500.7-R](#), Joint Ethics Regulation